

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA

Alexandria Division

UNITED STATES OF AMERICA

v.

KEVIN MCAVENIA,

Defendant.

Case No. 1:22-CR-86

The Honorable Leonie M. Brinkema

STATEMENT OF FACTS

The United States and the defendant, KEVIN MCAVENIA, agree that the United States would have proven at trial beyond a reasonable doubt and with admissible and credible evidence that, from at least on or about July 26, 2021, through on or about January 8, 2022, within the Eastern District of Virginia and elsewhere, the defendant used a means or facility of interstate or foreign commerce to knowingly receive visual depictions of minors engaging in sexually explicit conduct, as defined in 18 U.S.C. § 2256(1) & (2), the production of which involved the use of a minor engaging in such conduct.

The United States and the defendant further agree that the United States also would have proven at trial beyond a reasonable doubt and with admissible and credible evidence that, on or about January 14, 2022, in Arlington, Virginia, within the Eastern District of Virginia, the defendant knowingly possessed at least one matter containing one or more visual depictions that had been shipped or transported using any means or facility of interstate or foreign commerce, or in or affecting interstate or foreign commerce, and the production of such visual depictions involved the use of a minor engaging in sexually explicit conduct and such visual depictions were of such conduct.

The United States and the defendant further agree that the following facts are true and correct, and that had this matter proceeded to trial, the United States would have proven them beyond a reasonable doubt with admissible and credible evidence:

1. From at least on or about December 11, 2020 through on or about January 3, 2021, the defendant, using his laptop computer and the kmcavenia@gmail.com account, uploaded via the Internet hundreds of electronic files depicting minors engaging in sexually explicit conduct to his Google Drive, which was a cloud-based storage account. By uploading these files to his Google Drive, the defendant transported the files from his home in Arlington, Virginia, within the Eastern District of Virginia, to Google's servers.

2. In or around November 2021, a search warrant was executed on the kmcavenia@gmail.com account. That search revealed that the defendant stored within his Google Drive hundreds of video and image files depicting minors engaging in sexually explicit conduct. Among the minors depicted in those files were prepubescent females engaging in bestiality and prepubescent males and females engaging in vaginal and oral sex.

3. On January 14, 2022, law enforcement executed a federal search warrant at the defendant's residence in Arlington, Virginia. During the residential search, law enforcement seized multiple digital media and devices, including: (a) a Lenovo Thinkpad X1 laptop computer (S/N: PF-27XCXY) (hereinafter, "the Laptop"); (b) an Intel Processor desktop computer (S/N: BTHN02300729) (hereinafter, "the Desktop"); and (c) a Synology Network Attached Storage device (S/N: 2140RLRM5QNT) (hereinafter, "the NAS").

4. Each of the three devices described in Paragraph 3 was manufactured outside of the Commonwealth of Virginia, and thus had, at the time of the seizure, been shipped or transported in interstate or foreign commerce. Moreover, each device belonged to the defendant and was used

solely by him.

5. During the execution of the search warrant, law enforcement encountered the defendant at the residence. The defendant knowingly and voluntarily agreed to speak to law enforcement at the Arlington County Police Department in a non-custodial setting. The defendant was nonetheless advised of his *Miranda* rights, which he waived.

6. During the interview, the defendant admitted that his interest in downloading and viewing child pornography began over 20 years ago when he was in middle school. The defendant explained that he used to download child pornography using peer-to-peer file sharing networks, but that more recently he had been downloading child pornography files to his Laptop using The Onion Router (TOR). The defendant admitted that, over the course of several years, he had downloaded and saved thousands of child pornography files. He confirmed that he used the kmcavenia@gmail.com account and that it was deactivated at some point, but that child pornography had been saved within the Google Drive associated with his Gmail account. He also admitted that he would use the Desktop and the NAS as backup storage for his Laptop, and that child pornography would be found on those devices.

7. After the residential search, law enforcement conducted a digital forensic examination of the devices seized from the defendant's residence. The digital forensic examination confirmed the defendant's statements. The digital forensic analysis revealed that, across the three devices, at least 6,800 video and image files depicted minors engaging in sexually explicit conduct. The majority of those files were video files, amounting to over 21 hours of child sexual abuse material on the Laptop and Desktop alone. Among the depictions of minors engaging in sexually explicit conduct within the files were depictions of prepubescent minors and minors who had not attained the age of 12 years, depictions of sadistic or masochistic conduct, and

depictions of the sexual abuse and exploitation of a toddler. Several examples are as follows:

- a. A video, titled in part, “3y girl . . . molested by . . . sexy babysitter.” This approximately 39-minute video file depicts a female toddler performing oral sex and digital penetration on an adult female, as well as an adult female performing oral sex and digitally penetrating the toddler.
- b. A video, titled in part, “pthc . . . 10Yo And 12Yo Girls Play With 14Yo Boy.”¹ This approximately 20-minute video file depicts two nude prepubescent females performing sexual acts with each other on a couch, including oral sex. Later, a nude pubescent minor male enters the picture and the prepubescent minor females perform oral sex on the minor male, followed by the minor male rubbing and attempting to insert his erect penis into the vagina of the younger prepubescent female.
- c. A video, titled in part, “12yo . . . fuckbeads.” This video file, approximately 3 minutes and 34 seconds, depicts a nude adult male inserting anal beads into the anus of a nude pubescent minor female. The adult male then begins having vaginal sex with the nude pubescent minor female while continuing to force additional anal beads into the minor female’s anus.
- d. A collection of 258 image and video files of the same 15-year-old female (titled, in part, “Incest Whore”), more than 60 of which depict the minor female engaging in sexually explicit conduct. Some of the sexually explicit acts include lascivious displays of her vagina and anus, masturbation while self-gagging, and performing oral sex on a minor pubescent male. Certain videos also depict the minor female defecating on a bathroom floor, rubbing the feces all over her body and eating the feces,

¹ “Pthc” is a known acronym among child-pornography offenders for “pre-teen hardcore.”

and then masturbating with the feces; she appears to be crying at times and under duress.

8. The digital forensic analysis of the Laptop revealed that the defendant accessed the TOR browser to download child pornography files from at least on or about July 26, 2021, through on or about January 8, 2022. The defendant downloaded these files to his Laptop while at his home in the Eastern District of Virginia. The defendant then stored these files in two specific folder locations on the Laptop: *C:\Users\kmca\Downloads* and *C:\Users\kmca\MISC*. The Laptop also contained a folder *C:\Users\kmca\Google Drive\MISC\Stuff*, from where the defendant uploaded child pornography to his Google Drive account.

9. The defendant viewed the images and videos depicting minors engaging in sexually explicit conduct that he downloaded. For instance, a review of the list of VLC Recently Played Files revealed 30 video files, all of which depict minors engaging in sexually explicit conduct, that had been played using the VLC media player software on the Laptop just days prior to the residential search.

10. The digital forensic examinations of the Desktop and the NAS revealed that the defendant used both devices to store child pornography files. The defendant transferred onto the NAS and the Desktop numerous child pornography files that he had originally downloaded onto the Laptop using the Internet. For instance, files depicting minors engaging in sexually explicit conduct were found in two locations on the Desktop: *C:\Users\kmca\Pictures\Saved Pictures\MISC* and *C:\Users\kmca\Downloads*. Likewise, files depicting minors engaging in sexually explicit conduct were found on the NAS in, among other places, the “master backup” folder for kevin-laptop (the name of the Laptop). Examples of such files include:

- a. The video titled, in part, “belt.” This approximately 16-minute video file depicts a

pubescent minor female nude in the bathroom, with a belt tightened around her neck, masturbating with a hairbrush and two toothbrushes.

b. The video titled with reference to incest between a 14-year-old and a four-year-old.

This approximately 14-minute video file depicts a pubescent minor male masturbating in front of a computer. Several times during the video a partially clothed prepubescent female is forced to rub the erect penis of the minor male and insert his penis into her mouth. The minor male lasciviously displays the prepubescent female's exposed vagina to the camera and on multiple occasions attempts to insert his erect penis into the prepubescent female's vagina.

c. The video titled, in part, "13yo . . . whoreslave." This approximately 1-minute, 45-second video file depicts a nude pubescent female on her knees with her hands behind her back and her mouth wide open. A nude adult male enters the picture and forces the pubescent female to perform oral sex on his erect penis, gagging her multiple times.

11. Throughout the time of the offense conduct, the defendant held a Top Secret security clearance and was working as a contractor for the U.S. Government. In that position, he provided support to federal agencies in chemical, biological, radiological, and nuclear responses and emergency management.

* * * * *

12. This Statement of Facts includes those facts necessary to support the plea agreement between the defendant and the United States. It does not include each and every fact known to the defendant or to the United States, and it is not intended to be a full enumeration of all of the facts surrounding the defendant's case.

13. The actions of the defendant, as recounted above, were in all respects knowing and deliberate, and were not committed by mistake, accident, or other innocent reason.

Respectfully submitted,

Jessica D. Aber
United States Attorney

Date: July 28, 2022

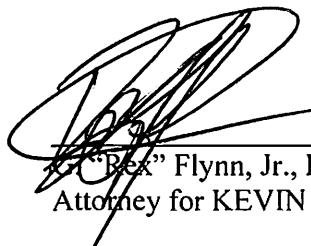
By: 
Rachel L. Rothberg
Special Assistant United States Attorney (LT)
Laura D. Withers
Assistant United States Attorney

After consulting with my attorney and pursuant to the plea agreement entered into this day between the defendant, KEVIN MCAVENIA, and the United States, I hereby stipulate that the above Statement of Facts is true and accurate, and that had the matter proceeded to trial, the United States would have proved the same beyond a reasonable doubt.



KEVIN MCAVENIA

I am G. "Rex" Flynn, Jr., the defendant's attorney. I have carefully reviewed the above Statement of Facts with him. To my knowledge, his decision to stipulate to these facts is an informed and voluntary one.



"Rex" Flynn, Jr., Esq.
Attorney for KEVIN MCAVENIA